ACTION ITEM # 1

MEMORANDUM:

SUBJECT: SECURITY RELATED INFORMATIONAL MATERIAL
FOR ALL AIRS USERS

FROM: MICHAEL W. HAMLIN

PURPOSE

This informational material was developed to outline briefly the security measures for the AIRS system and to explain why these measures were developed, and to request the support of all AIRS users in complying with these measures. The security measures for AIRS are intended to protect the air quality, emissions and compliance data that State and local agencies periodically submit to EPA. This protection includes unauthorized modification or loss of data, while at the same time protecting the underlying computer system that EPA operates.

The AIRS application (and the data it contains) supports EPA, as well as State and local agencies needing information to carry out air quality management programs. All AIRS users must ensure that the AIRS application and its data are protected from loss, misuse, and unauthorized access or modification. It is also paramount that any sensitive information (e.g., enforcement, compliance) in the AIRS application is protected from unauthorized access.

EPA's Security Measures for AIRS

The AIRS, which consists of two major subsystems, Air Quality Subsystem (AQS) and Air Facility Subsystem (AFS), is a ADABAS database management system located on EPA's National Computer Center (NCC) mainframe. As such, AIRS follows the security procedures set forth by the NCC which primarily involves the use of user accounts, user ids, passwords and ADABAS/Natural Security. Briefly, these procedures require that:

a. Any individual wanting to be able to access data in the AIRS data base must be given authorization to use a mainframe account and obtain an NCC user id. The id and a secure password (determined by the user) must be used when accessing the NCC mainframe and AIRS data base. State and local agency users are given limited update authority (i.e., they may only add or modify data for their particular agency).

b. A user id is only assigned to an individual (rather than an agency) and only to an individual that is recommended for access by the State or local agency (in writing) and approved by the appropriate EPA Regional Office AIRS contact and Regional RACF Administrator. Individuals granted user ids have a responsibility to use their ids in an appropriate manner at all times and ensure that the access they have been personally granted is not shared with others (either deliberately or inadvertently).

AIRS Application Guidelines for All Users

There are certain security practices and procedures that should be followed to minimize the potential misuse or damage to the AIRS database. Some of these include:

General

- Be familiar with the security policies and practices involving the AIRS application, especially those for confidential or sensitive information (see AIRS Security Plan).

- Maintain security for the application by correctly using established security mechanisms (use of unique user id and password) and practices when accessing the AIRS application.

- Do not attempt to view, change, or delete data unless you are authorized to do so.

- Do not use your system privileges to obtain data/files or run applications for anyone who is not authorized to view or use data that are sensitive.

- Be alert to potential threats to corrupt or destroy AIRS application and database.

- Ensure that no one person has sole access to, or control over, AIRS information and processing resources.

- Guard user id and password. Do not loan out to others.

Sensitive Data

- Be sure to provide only authorized personnel with sensitive data (whether the data are on your screen or on paper).

- When viewing or processing confidential or sensitive data, be sure the PC is in a non-traffic area and that only persons authorized to see the data are in the area.

- Protect all documents and reports containing sensitive data. Be sure that they are labeled “sensitive.”

- Destroy sensitive documents when finished with them.

- Do not save sensitive data to your hard drive, diskette, or floppy.

- Log off your computer when you are to be away from your work station.

- Lock up or put away sensitive data.

Password Protection

- Control access to your PC. Log out whenever you leave your machine.

- Change your application password every 90 days. Use at least 8 characters in your application password.

- Use a mix of alpha and numeric characters.

- Do not use family names, birthdays, sports teams' names, or words that can be found in the dictionary.

- Do not use consecutive keys on a keyboard or all the same character.

- Use new passwords. Do not use the last 8 versions of your password.

- If you believe your password has been compromised, change it immediately.

- Memorize your password rather than writing it down somewhere.

Who To Notify

- Notify the AIRS Security Officer immediately of security incidents.

- Notify the AQS or AFS application manager (Jake Summers (AQS) at 919-541-5695 or Chuck Isbell (AFS) at 919-541-5448) when staff have been terminated or changed positions to have their access to the application terminated.

Summary

This information was compiled to assure that the contents and integrity of AIRS data will be secure. In order to maintain security for the data provided in AIRS, we suggest that the guidelines above be followed. The security measures that have been established are designed to protect the data that State and local agencies submit, while at the same time protecting the computer systems that EPA operates.

Any questions concerning the above information should be referred to Michael Hamlin, AIRS Security Officer, at (919) 541-5232.